# METHOD FOR SUPPLYING CYRPTOGRAPHIC ALGORITHM CONSTANTS TO A STORAGE-CONSTRAINED TARGET

ABSTRACT

The present invention provides for authenticating a message. A security function is performed upon the message. The message is sent to a target. The output of the security function is sent to the target. At least one publicly known constant is sent to the target. The received message is authenticated as a function of at least a shared key, the received publicly known constants, the security function, the received message, and the output of the security function. If the output of the security function received by the target is the same as the output generated as a function of at least the received message, the received publicly known constants, the security function, and the shared key, neither the message nor the constants have been altered.